

REMARKS

This Amendment is fully responsive to the final Office Action dated October 9, 2009, issued in connection with the above-identified application. With this Amendment, claims 1, 2, 5, 10-12 and 14-17 have been canceled without prejudice or disclaimer to the subject matter therein, and claims 18-39 have been added. No new matter has been introduced by the new claims added. Favorable reconsideration is respectfully requested.

I. Interview Summary

At the outset, the Applicants thank Examiner Vaughan for granting the telephone interview (hereafter "interview") with the Applicants' representative, which was conducted on December 21, 2009.

During the interview, the present invention and the cited prior art were discussed in detail. Specifically, two different options for amending the independent claims were discussed.

It was agreed that the second option for amending the independent claims would be best for distinguishing the present invention from the cited prior art. It was noted that the present invention (i.e., in the second option) was distinguishable from the cited prior art in that a key generation unit performs a predetermined operation using the first and second keys, generates a part of a result of the predetermined operation as a first encryption key and generates another part of the result as a first hash key. Accordingly, in the present invention, it is not necessary to perform an additional calculation to generate the first encryption key and the first hash key.

On the other hand, Morais lacks any disclosure of the following features: 1) performing a predetermined operation using first and second keys; 2) generating a part of a result of the predetermined operation as a first encryption key; and 3) generating another part of the result as a first hash key. Morais indicates that "the generator 410 may create keys," however, an additional operation is performed. Moreover, neither Diffie nor Bellare disclose or suggest the features of the key generation unit of the present invention noted above.

At the conclusion of the interview, the Examiner indicated that the claim amendments (i.e., as presented in the second option) should distinguish the present invention from the cited prior art, and further consideration would be given to the claim amendments upon the filing of a

formal response to the Office Action.

II. Rejections under 35 U.S.C. 112

In the Office Action, claim 5 has been rejected under 35 U.S.C. 112, second paragraph, as being indefinite. In particular, the Examiner alleges that the features of claim 5 contradict the features of the claim from which it depends. Claim 5 has been canceled thereby rendering the above rejection under 35 U.S.C. 112 to that claim moot.

III. Rejections under 35 U.S.C. 103

In the Office Action, claims 1, 2, 5, 10-12 and 14-17 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Diffie et al. (U.S. Patent No. 5,371,794, hereafter “Diffie”) in view of Morais et al. (U.S. Publication No. 2003/0093669, hereafter “Morais”), and further in view of Bellare et al. (an article entitled “Keying Hash Functions for Message Authentication,” 1996 publication, hereafter “Bellare”).

Claims 1, 2, 5, 10-12 and 14-17 have been canceled without prejudice or disclaimer to the subject matter therein. Additionally, claims 18-39 have been added. New independent claims 18, 19, 22 and 23 include features that are consistent with the claim amendments (i.e., in the second option) proposed during the interview conducted on December 21, 2009. Given the extent of the proposed amendments (i.e., in the second option), the Applicants determined that it was more efficient to replace the pending claims with new claims 18-39.

Accordingly, independent claims 18, 19, 22 and 23 are believed to distinguishable from the cited prior art for similar reasons noted during the interview conducted on December 21, 2009. That is, independent claim 18 recites the following features:

“[a]n encrypted communication system comprising:

a first device; and

a second device, wherein

said first device includes:

a first data generation unit operable to encrypt a first key using a public key of said second device to generate first encrypted key data, and transmit the first encrypted key data to said second device;

a first decryption unit operable to receive, from said second device, second encrypted key data generated by said second device encrypting a third key using a public key of said first device, and decrypt the second encrypted key data using a private key of said first device to obtain a second key;

a first key generation unit operable to perform a predetermined operation using the first and second keys, generate a part of a result of the predetermined operation as a first encryption key and generate another part of the result as a first hash key; and

a first communication unit operable to encrypt first transmission data using the first encryption key to generate first encrypted data, apply a one-way operation to the first transmission data using the first hash key to calculate a first detection value for tamper detection to be performed on the first encrypted data by said second device, and transmit the first encrypted data and the first detection value to said second device, and

said second device includes:

a second data generation unit operable to encrypt the third key using the public key of said first device to generate the second encrypted key data, and transmit the second encrypted key data to said first device;

a second decryption unit operable to receive, from said first device, the first encrypted key data generated by said first device encrypting the first key using the public key of said second device, and decrypt the first encrypted key data using a private key of said second device to obtain a fourth key;

a second key generation unit operable to perform the predetermined operation using the third and fourth keys, generate a part of a result of the predetermined operation as a second encryption key and generate another part of the result as a second hash key; and

a second communication unit operable to receive the first encrypted data and the first detection value, decrypt the first encrypted data using the second encryption key to generate second transmission data, apply a one-way operation to the second transmission data using the second hash key to calculate a second detection value, compare the first and second detection values, and when the first and second detection values match, recognize the second transmission

data as valid, and when the first and second detection values do not match, recognize the second transmission data as invalid.” (Emphasis added).

The features emphasized above in independent claim 18 are similarly recited in independent claims 19, 22 and 23. Specifically, independent claim 19 is a communication device that includes “a key generation unit” having the same features of the “first key generation unit” of independent claim 18. Independent claim 22 is a corresponding method and claim 23 is a corresponding computer program, and both claims include steps directed to the features of the “key generation unit” of independent claim 18.

Additionally, the features emphasized above in independent claim 18 (and similarly recited in independent claims 19, 22 and 23) are fully supported by the Applicants’ disclosure (see e.g., pgs. 10-11; pgs. 19; and pgs. 29-30).

The present invention (as recited in independent claims 18, 19, 22 and 23) is distinguishable from the cited prior art in that a key generation unit performs a predetermined operation using the first and second keys, generates a part of a result of the predetermined operation as a first encryption key and generates another part of the result as a first hash key. Accordingly, it is not necessary to perform an additional calculation to generate the first encryption key and the first hash key.

In the Office Action, the Examiner relied on Diffie, Morais and Bellare for disclosing or suggesting all the features of the present invention. However, for similar reasons noted during the interview conducted on December 21, 2009, Diffie, Morais and Bellare fail to disclose or suggest the features (noted above) recited at least in independent claims 18, 19, 22 and 23.

Diffie discloses that “[t]he Mobile 100 generates another random number RN2 and will use the value (RN1 xor RN2) as the session key” (see col. 8, lines 45-47). However, Diffie fails to disclose all the features of the key generation unit of the present invention (as recited in independent claims 18, 19, 22 and 23).

That is, with use of the technique disclosed by Diffie, a part of an operation result cannot be generated as the first encryption key, and another part of the operation result cannot be generated as the first hash key.

Morais discloses in ¶[0045] a LAN key generator 406 that uses the console-based key 402 and the title-based key 404 to derive a LAN key 408. In one embodiment, the LAN key generator 406 computes a one-way cryptographic function using the two keys 402 and 404 during a network stack initialization.

As one example of a suitable cryptographic function, in Moraes, the LAN key generator 406 concatenates the keys 402 and 404 and performs an HMAC-SHA-1 (Hashed Message Authentication Code--Secure Hash Algorithm 1) operation on them to produce the LAN key 408.

As described in ¶[0046] of Moraes, the LAN key 408 is then used to produce shared secret keys. Specifically, when the network stack is initialized, a broadcast key generator 410 uses the LAN key 408 to generate a title broadcast encryption key 412 and a title broadcast signature key 414. For example, the generator 410 may create keys for symmetric ciphers, asymmetric ciphers, hashing algorithms, and digest algorithms.

In other words, according to Moraes, a LAN key 408 is generated using the console-based key 402 and the title-based key 404. After that, Moraes discloses that a title broadcast encryption key 412 and a title broadcast signature key 414 are generated from the LAN key 408 with use of symmetric ciphers, asymmetric ciphers, hashing algorithms, and digest algorithms.

However, Moraes lacks any disclosure regarding the following features: 1) performing a predetermined operation using the first and second keys; 2) generating a part of a result of the predetermined operation as a first encryption key; and 3) generating another part of the result as a first hash key.

The technique disclosed by Moraes indicates that “the generator 410 may create keys.” However, in Moraes, an additional operation is performed.

In contrast, in the present invention (as recited in independent claims 18, 19, 22 and 23), because the key generation unit generates a part of its operation result as the first encryption key, and generates the other part as the first hash key, an additional operation is not required.

Bellare discloses a MAC algorithm. Also, Bellare discloses a compression function in Fig. 1 on p. 8. However, Bellare also fails to disclose all the features of the key generation unit

of the present invention. Consequently, with use of the technique disclosed by Bellare, while one key can be generated from two random numbers, neither part of a computation result can be generated as the first encryption key nor another part of the computation result as the first hash key.

As noted above, the present invention (as recited in independent claims 18, 19, 22 and 23) performs a predetermined operation using the first and second keys, generates a part of a result of the predetermined operation as a first encryption key and generates another part of the result as a first hash key. Accordingly, there is no need to perform an additional operation to generate the first encryption key and the first hash key.

Accordingly, no combination of Diffie, Morais and Bellare would result in, or otherwise render obvious, independent claims 18, 19, 22 and 23. Likewise, no combination of Diffie, Morais and Bellare would result in, or otherwise render obvious, claims 20, 21 and 24-39 at least by virtue of their respective dependencies from independent claims 18, 19, 22 and 23.

IV. Conclusion

In light of the above, the Applicants submit that all the pending claims are patentable over the prior art of record. The Applicants respectfully request that the Examiner withdraw the rejections presented in the outstanding Office Action, and pass the present application to issue. The Examiner is invited to contact the undersigned attorney by telephone to resolve any remaining issues.

Respectfully submitted,

Yuichi FUTA et al.

/Mark D. Pratt/
By: 2010.01.04 14:14:19 -05'00'

Mark D. Pratt
Registration No. 45,794
Attorney for Applicants

MDP/ats
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
January 4, 2010